ALGORITMA: Jurnal Ilmu Komputer dan Informatika
Volume: 02, Number : 01, April 2018 ISSN 2598-6341 (online)

Pengamanan Berkas Dokumen Menggunakan Fungsi Algoritma Steganografi LSB

Indra Gunawan[1], Sumarno[2], Eka Irawan[3], Heru Satria Tambunan[4]
[1,2,3,4]STIKOM Tunas Bangsa
[1,2]Program Studi Teknik Informatika, [3,4]Program Studi Sistem Informasi
Pematangsiantar, Indonesia
[1]indra@amiktunasbangsa.ac.id, [2]sumarno@amiktunasbangsa.ac.id, [3]eka.irawan@amiktunasbangsa.ac.id,
[4]heru@amiktunasbangsa.ac.id

Abstrak

Didalam Dunia Teknologi Informasi ilmu komputer, pengamanan data sesuatu hal yang sangat penting supaya data tidak dapat disalah gunakan beberapa pihak yang belum/bukan memiliki hak. Dalam pengiriman berkas dokumen sangatlah dibutuhkan suatu pengamanan supaya berkas dokumen tersebut bisa diterima oleh yang memiliki hak untuk menerimanya. Oleh karena itu sangatlah didibutuhkan suatu proses penyandian/enkripsi berkas dokumen. Diantar ilmu kriptografi yang dapat mengamankan berkas dokumen tersebut diantaranya Algoritma Steganografi LSB (*Least Significant Bit*). Analisa ini bertujuan untuk meningkatkan pengamanan berkas dokumen dengan cara menyandikan sebuah berkas dokumen tersebut, lalu memberikan sebuah sandi kedalam berkas dokumen tersebut.

Kata kunci : Enkripsi, Keamanan Data, Steganografi LSB, Berkas, Dokumen

Abstract

In the World of Information Technology computer science, data security something that is very important so that data can not be misused by some parties who have not / not have rights. In the delivery of documents documents is needed a security so that the document file can be accepted by those who have the right to receive it. It is therefore very necessary to process a document encryption / encryption file. Among the science of cryptography that can secure the document file such as LSB Steganography Algorithm (Least Significant Bit). This analysis aims to improve the security of document files by encoding a document file, then providing a password into the document file.

Keywords : *Encryption, Data Security, LSB Steganography, Files, Documents*

1. PENDAHULUAN

Menjaga keamanan data selalu menjadi masalah didalam ilmu komputer. Terlebih lagi bagaimana sesorang yang tidak memiliki hak akses, dapat melakukan pembobolan data, terutama data pesan teks dan video. Hal ini dapat memicu kasalah pahaman antara sipengirim dan sipenerima. Mekanisme yang sering dilakukan adalah dengan menggunakan metode yang paling sederhana, yaitu brute force attack sebagai media penyerangan [Gunawan, I. September 2016).

Didalam pengamanan suatu berkas dokumen, sangatlah dibutuhkan menggunakan sebuah metode/algoritma ilmu kriptografi, agar berkas dokumen tersebut bisa terjamin keamanannya, diantara begitu banyaknya metode/algoritma yang dapat dijadikan pengaman berkas dokumen tersebut adalah algoritma Steganografi (*Least Significant Bit*).

Algoritma steganografi mempunyai metode yang bisa digunakan seperti LSB (*Least Significant Bit*) dan EOF (*End Of File*). Kedua algoritma ini mempunyai model yang sangat berbeda dalam proses penyamaran dan penyembunyian data [Gunawan, I. Maret 2018]. Lain dari itu, algoritma ini juga masih digunakan untuk pengembangan didalam ilmu steganografi itu sendiri agar dapat menghasilkan model-model terbaru dari algoritma steganografi. Dalam penelitian sebelumnya dengan judul Pangamanan Acakan BISS menggunakan Algoritma RSA [Gunawan, I. Juli 2017], telah dijelaskan tentang bagaimana proses penyisipan teks kedalam sebuah video, lalu mengacaknya, akan tetapi akan terlihat perbedaan yang sangat jauh dari segi ukuran video yang sudah disisipkan oleh teks.

Dengan meningkatkan sistem keamanan dari berkas dokumen dapat membantu mengamankan data-data yang ada didalam berkas dokumen pada saat proses pengiriman data, sehingga berkas dokumen

tersebut dapat dengan selamat sampai kepada si penerima/yang memiliki hak untuk membuka berkas dokumen tersebut.

Steganografi (*steganography*) berasal dari bahasa yunani yaitu *steganos* yang memiliki arti tersembunyi dan *graphein* yang berarti menulis, sehingga jika disatukan, maka artinya adalah "menulis tulisan yang tersembunyi" [Dony, A. 2009]. Istilah lainnnya, steganografi adalah sebuah seni atau sebuah ilmu yang diimplementasikan untuk menyisipkan pesan rahasia dengan berbagai cara, sehingga hanya orang yang dituju saja yang dapat mengetahui maksud dan tujuan dari pesan tersebut.

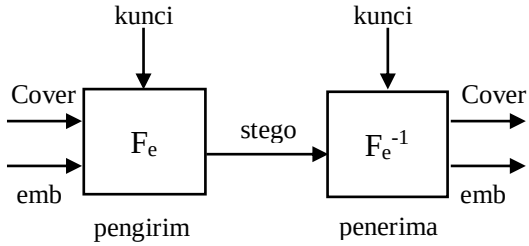
Dalam metode/algoritma steganografi, memiliki beberapa kriteria yang harus dimiliki, diantaranya [Vembrina, Y. 2006] :

1. *Impercepbility*
   Keberadaan pesan tidak dapat dipersepsi oleh indra manusia, baik indra pendengaran maupun indra penglihatan.
2. *Fidelity*
   Mutu dari citra penampung tidak jauh berubah. Setelah penambahan pesan rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau didalam citra tersebut masih terdapat teks rahasia.
3. *Recovery*
   Pesan rahasia yang disembunyikan didalam citra digital harus dapat diungkapkan kembali seperti aslinya.

Ada juga beberapa istilah yang lain yang ada kaitan eratnya dengan steganografi, diantaranya:

1. *Hident Text* atau *embedded message* : pesan yang disembunyikan
2. *Covertext* atau *Cover-Object* : pesan yang digunakan untuk menyembunyikan pesan yang sudah tersembunyi (*embedded message*)
3. *Stegotext* atau *stego-object* : pesan yang sudah berisi pesan tersembunyi (*embedded message*).

Steganografi yang menggunakan media gambar *hiddent text* atau *embedded text* yang sudah disisipkan merupakan pesan yang akan disisipkan kedalam *convertext* atau *coverobject*, yaitu berkas dokumen yang digunakan sebagai media penampung berkas kedalam dokumen gambar yang dihasilkan *stegotext* atau *stego-object* yang merupakan sebuah file gambar yang memiliki pesan *embedded*.



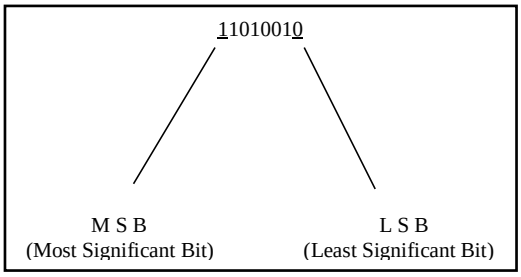
Gambar 1. Sistem Steganografi [Gunawan, I. Maret 2018]

Untuk Proses Penyandian dari pada berkas dokumen ke dalam sebuah *Cover* dinyatakan sebagai *encoding*. Untuk pemisahan/ekstraksi sandi dari berkas dokumen disebut juga sebagai stego dan dinamakan sebagai *decoding*. Dari kedua proses ini akan membutuhkan kunci rahasia (*private* key) agar hanya satu pihak saja yang memiliki hak dan yang dapat melakukan proses enkripsi berkas dokumen seperti yang dijelaskan pada gambar 1.

Pada dasarnya didalam algoritma kriptografi steganografi, terdapat 6 (enam) teknik yang yang digunakan [Dony, A. 2009]:

1. *Injection* (Penanaman) merupakan suatu teknik yang menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya, sehingga mudah dideteksi. Teknik ini sering juga disebut dengan *embedded*.
2. Subsitusi data normal digantikan dengan data rahasia. Biasanya hasil teknik itu tidak perlu mengubah ukuran data asli, akan tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas dari media yang ditumpangi.
3. *Transform domain* (transformasi domain) teknik ini sangat efektif. Pada dasarnya transformasi domain menyembunyikan data pada "*transform space*".
4. *Spread Spectrum* sebuah teknik pentransmisian menggunakan *Pseudo-noise code*, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi signal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar dari pada sinyal jalur komunikasi telekomunikasi.
5. *Statistical Method* teknik ini disebut juga skema *steganograpic* 1 bit. Skema tersebut menanamkan 1 bit informasi pada media tumpangan dan mengubah statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0.
6. *Distortion Metode* ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.

Penyembunyian pesan dilakukan dengan merubah bit-bit didalam segmen citra dengan bit-bit pesan rahasia. Metode yang paling sering digunakan adalah dengan modifikasi LSB (*Least Significant Bit*) pada citra penampung. Pada susunan bit didalam sebuah byte, ada bit yang paling signifikan yang disebut MSB (*Most Significant Bit*) dan bit yang paling kurang significant atau LSB (*Least Significant Bit*).



Gambar 2. Sampel Susunan Bit pada LSB dan MSB [Gunawan, I. Maret 2018]

Contoh susunan Bit pada byte yang mendeskripsikan bit yang cocok untuk dirubah adalah bit LSB, karena pergantiannya hanya merubah nilai byte satu lebih tinggi atau lebih rendah dari nilai sebelumnya. Sampelnya byte didalam sebuah gambar dinyatakan sebuah warna tertentu, maka dilakukan perubahan pada bit LSB dan tidak akan mengganti warna secara signifikan. Sebelum melakukan pergantian bit-bit pada LSB, semua data citra harus dirubah terlebih dahulu kedalam format bit, jadi setiap data piksel dari gambar akan mengandung beberapa komponen warna merah, hijau dan biru (RGB) [Rahim, M. 2006].

Dengan memodifikasi susunan dari bit pada byte tersebut, tidak akan membuat suatu pengaruh yang sangat besar terhadap ukuran dari file dokumen, sehingga dengan melakukan modifikasi susunan dari bit pada byte tidak akan memperbesar ukuran daru kapasitas berkas dokumen.

Metode EOF adalah beberapa metode yang masih digunakan didalam algoritma steganografi. Metode ini menggunakan cara dengan melampirkan data pada akhir file. Sehingga tidak akan mempengaruhi kualitas data awal yang akan dilampirkan pesan. Akan tetapi ukuran file yang telah dilampirkan pesan rahasia akan sedikit bertambah dari ukuran sebelumnya [Agustaviana, I. 2012].

Walaupun metode ini sudah sedikit kuno, tetapi metode ini masih sangatlah ampuh untuk dijadikan salah satu pengamanan sebuah data, terutama pengaman berkas dokumen.

Metode EOF menggunakan kelemahan indera manusia yang tidak sensitif, sehingga seolah-olah tidak memiliki perbedaan bila dilihat pesan tersebut apakah sudah disisipkan atau belum [Edisuryana, M. 2013].

Didalam Metode EOF pesan teks yang akan dilampirkan pada media akan dikonversi terlebih dahulu kedalam bilangan nilai desimal berdasarkan yang tertera pada tabel ascii. Kode ascii (*American Standart Code for Information Interchange*) adalah representasi numerik dari karakter-karakter yang digunakan pada komputer dengan ketentuan huruf a-z, A-Z, 0-9 dan simbol standart yang tertera pada *keyboard*.

Berkas merupakan kumpulan dari beberap informasi yang sudah dilakukan perekaman data dan disimpan didalam sebuah media penyimpanan data. Sedangkan dokumen merupakan suatu tulisan yang memuat sebuah informasi.

Masalah dalam pengamanan data masih merupanan suatu aspek penting didalam penjagaan penyimpanan data, terutama contoh data yang dipakai atau disisipkan kedalam bentuk digital. Hal ini disebabkan karena kemajuan yang sangat pesat didalam bidang ilmu komputer dengan konsep *open-system* yang sudah banyak digunakan, sehingga hal ini dapat memudahkan seseorang untuk melakukan perusakan data terutama contoh data yang dipakai atau disisipkan kedalam bentuk digital tanpa harus diketahui oleh pihak penyimpan data [Gunawan, I. Maret 2018]. Oleh karena itu dibutuhkan pengelolaan kemaanan data digital dengan menggunakan sebuah algoritma kriptografi, salah satunya yaitu algoritma steganografi Least Significant Bit (LSB).

2. IMPLEMENTASI

Berdasarkan dari beberapa teoritis yang sudah dijelaskan dan dibahas, untuk proses enkripsi data dengan memakai algoritma kriptografi steganografi LSB, sangatlah dibutuhkan sampel data bilangan untuk dapat menampung karakter-karakter yang berikutnya dikonversi kembali kedalam bilangan biner.

Untuk proses-proses atau *Pseuducode* yang digunanakan adalah :

Proses Enkripsi :

```
k = 1;
   for i = 1 : height
      for j = 1 : width
         LSB = mod(double(c(i,j)), 2);
        if (k>m || LSB == b(k))
           s(i,j) = c(i,j);
        else
           if(LSB == 1)
              s(i,j) = c(i,j) - 1;
           else
              s(i,j) = c(i,j) + 1;
           end
        k = k + 1;
     end
     end
```

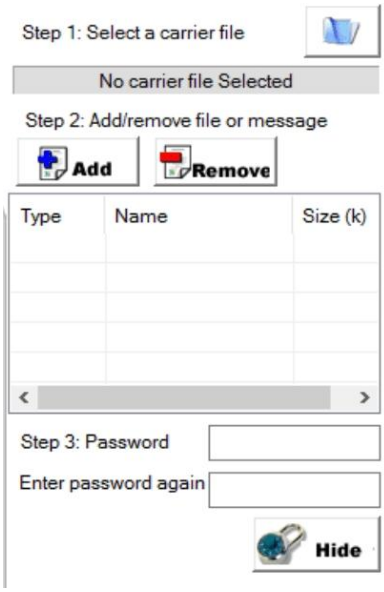
Proses Dekripsi :

```
k = 1;
   for i = 1 : height
      for j = 1 : width
         if (k <= m)
            b(k) = mod(double(s(i,j)),2);
            k = k + 1;
         end
```

```
    end
end
```

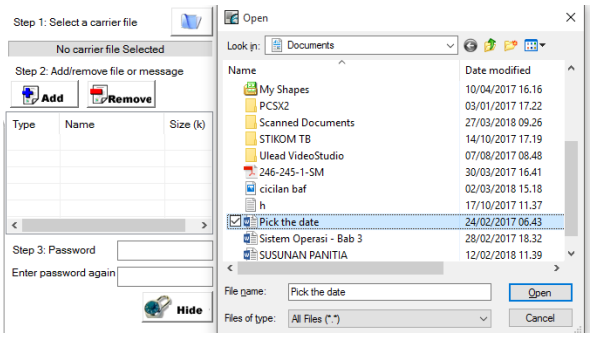
3. HASIL

Untuk tahap ini, akan dihasilkan proses untuk memulai langkah-langkah dalam pengamanan berkas dokumen. Berkas dokumen akan dipilih sebagai sampel dan diamanankan dengan cara memproteksikan file dokumen dan memberikan sebuah sandi.



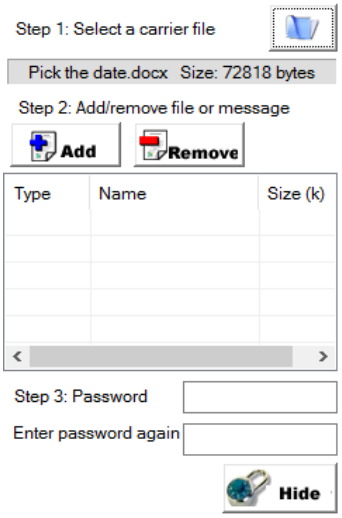
Gambar 3. Tampilan Sistem

Dari Gambar 3, merupakan tampilan awal dari sebuah sistem yang akan digunakan untuk proses pengamanan berkas dokumen.



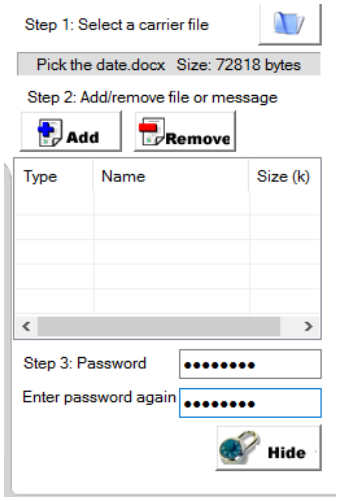
Gambar 4. Proses Pemilihan berkas dokumen

Dari Gambar 4, proses pemilihan berkas dokumen yang akan di sandikan.



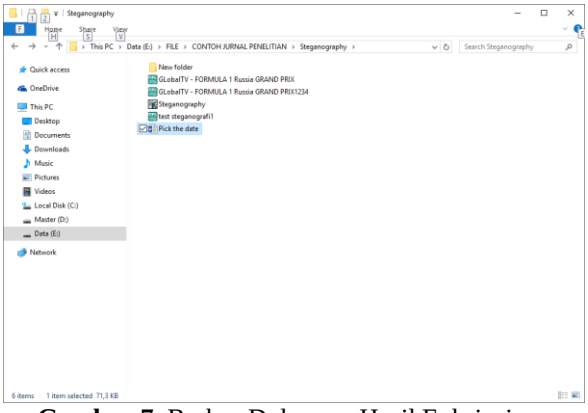
Gambar 5. Berkas yang sudah dipilih

Dari gambar 5, berkas dokumen yang sudah dipilih akanakan terleksi berdasarkan nama file dan ukurannya.



Gambar 6. Proses Pemberian Kata Sandi

Dari Gambar 6, proses pemberian kata sandi kedalam berkas dokumen akan disisipkan kedalam berkas dokumen.



Gambar 7. Berkas Dokumen Hasil Enkripsi

4. KESIMPULAN

Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit dapat digunakan untuk memberikan pengamanan terhadap file video yang disisipkan oleh pesan teks, sehingga dengan menggunakan algoritma kriptografi steganografi LSB, bisa dijadikan sebagai suatu cara untuk memberikan pengaman terhadap file vidieo yang akan dikirim kepada sipenerima.

5. DAFTAR PUSTAKA

Agustaviana, I. Aplikasi Pesan Rahasia Berbasis Web Menggunakan Vigenere Cipher dan Steganografi EOF. Skripsi Universitas Mulawarman. 2012.

Dony, A. Kemanan Multimedia. Yogyakarta : Andi. 2009.

Edisuryana, M., Isnanto, R.R. & Somantri, M. "Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan Metode End Of File". Jurnal Teknik Elektro. Universitas Diponegoro Semarang. 2013.

Gunawan, I. "Penggunaan Bruto Force Attack dalam Penerapanya Pada Crypt8 Dan CSA-Rainbow Tool Untuk Mencari BISS". Jurnal Nasional Informatika danTeknologi Jaringan (InfoTekjar). Vol 1, No 1, pp. 52-55, September 2016.

Gunawan, I. "Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video". Jurnal Sains Komputer & Informatika (J-SAKTI). Vol 2. No. 1, pp. 57-65, Maret 2018.

Gunawan, I. "Pengamanan Acakan BISS Menggunakan Algoritma RSA". Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK). Vol. 2, pp. 58-63. Juli 2017.

Gunawan, I. "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA Untuk Pengamanan File Dokumen Dan Pesan Teks". Jurnal Nasional Informatika dan Teknologi Jaringan (InfoTekjar). Vol. 2, No. 2. Maret 2018.

Ida Ayu Laksmini Dewi. Frame Rate Minimum Pada Video Tanpa Kompresi Menggunakan Normalized Frame Difference Sebagai Pendeskripsi Intensitas Gerak. Skripsi : Jurusan Teknik Elektro Fakultas Teknik Universitas Udayana. 2015.

Vembrina, Y. Spread Spectrum Steganograpy. Bandung : Sekolah Teknik Elektro dan Informatika. 2006.

Rahim, M. Teknik Penyembunyian Data Rahasia Dengan Menggunakan Citra Digital Sebagai Berkas Penampung. Semarang : Universitas Diponegoro. 2006.

Sutoyo, T. Tori Pengolahan Citra Digital. Yogyakarta : Andi. 2009.